The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society

December 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

bkl
BAE, KIM & LEE

Table of Contents

I. Introduction

Contemporary everyday life is increasingly permeated by digital information, whether by creating, consuming or depending on it. Most of our professional and private lives now rely to a large degree on digital interactions.[1] As a result, access to and the use of data, and in particular personal data, are key elements and drivers of the digital economy and society.[2] This has brought us to a significant inflection point on the issue of legitimising the processing of personal data in the wide range of contexts that are essential to our data-driven, AI-enabled digital products and services.[3] The time has come to seriously re-consider the status of consent as a privileged legal basis and to consider alternatives that are better suited for a wide range of essential data processing contexts. The most prominent among these alternatives are the "legitimate interest" and "contractual necessity" legal bases, which have found an equivalent in a number of jurisdictions. One example is Singapore, where revisions to their data protection framework include a legitimate interest exemption.

Drawing largely from the experience under the EU's General Data Protection Regulation (GDPR) and several EU digital laws, this paper makes the case for shifting away from over-reliance on consent and exploring, instead, other legal bases such as contractual necessity and legitimate interest. It argues that to ensure the viability and success of the digital economy and society, GDPR-style consent does not always have to be the go-to legal basis for an ever-expanding multitude of data processing scenarios where it is insufficient, ineffective, or impracticable.

The objective of this paper is to serve as a case study for law and policymakers in other jurisdictions looking to update their digital legislative frameworks, including those related to privacy and data protection.

The first part of this paper provides an overview of recent changes in the EU framework and the resulting challenges and explores the limitations of a consent-based model and its ramifications for the effective and beneficial use of personal data and the development and deployment of AI-driven applications. It provides suggestions for balancing the rights of all stakeholders in the digital economy fairly and efficiently and for providing meaningful privacy protection.

The second part of the paper applies this to the changes being considered in South Korea as a case study. It is important that jurisdictions looking to the EU for inspiration when revising their own digital legislation take a cautious approach and learn from the challenges that are emerging in the EU as a result of these overlapping digital laws and the oversized role they grant consent as a legal basis for processing.

1 According to the EU's Digital Economy and Society Index (DESI), the percentage of individuals ages 16–74 who have never used the internet sank from 43.2 % to 6.96% between 2005 and 2022.

2 CJEU, Bundeskartellamt, para 50.

3 The OECD suggests that data access and sharing of private sector data helps generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product; and the online advertising market alone in Europe is worth €96.9 billion.

II. Legislative developments under the EU's Digital Strategy

To propel the significant economic potential of data-driven digital tools and services, the European Commission released a digital strategy in 2020. The strategy envisioned a safe and trusted digital space for individuals and a level playing field for businesses that foster innovation, growth, and competitiveness in the EU.[4] This was quickly followed by a flurry of significant legislative initiatives to implement the strategy:[5]

- The Digital Markets Act ("DMA")[6] intends to ensure fairness and contestability[7] in digital markets;
- The Digital Services Act ("DSA")[8] aims to provide clearer and more standardised rules for digital content with expanded transparency requirements, rules around content moderation, online advertising and protection of minors online;
- The Data Governance Act ("DGA")[9] and Data Act[10] ("DA") are intended to lay a framework for extended access to data, including data generated through the use of IoT devices;
- The EU AI Act[11] is the first comprehensive global regulation to come into effect and establish rules for AI developers and deployers, prohibit certain applications, and establish obligations and requirements based on risk.[12]

These are only a few examples, but each of these laws is premised on and intends to further promote the uptake in generation, use and exchange of data, including personal data, with an expectation of substantial economic benefits for the EU. The Commission predicts that the data economy in Europe will increase by €528 billion after these new legislative proposals take effect.[13]

The tsunami of new digital legislation in the EU may, however, also have created some challenges that could ultimately undercut the strategic goals of the Commission. For example, in so far as these digital laws regulate processing activities involving personal data, they overlap with the GDPR. This has resulted in a number of inconsistencies, potential unintended consequences and legal uncertainties, including with respect to the role of consent as an appropriate legal basis for processing in certain contexts.[14]

The growing number of EU digital laws has also led to concerns about overregulation more broadly and their impact on digital

4 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

5 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

6 Digital Markets Act, proposed December 2020, entry into force November 2023.

7 "Contestability" means the ability to overcome barriers to entry into the market.

8 Digital Services Act, proposed December 2020, entry into force November 2022.

9 Data Governance Act, proposed November 2020, entry into force June 2022.

10 Data Act, proposed February 2022, entry into force January 2024.

11 AI Act, proposed April 2021, entry into force August 2024.

12 This represents only a selection of the proposals relevant to the digital economy issued since 2020.

13 Kumpula-Natri, M. (2021, April 13). Building a European data strategy. The Parliament Magazine.

14 CIPL Paper - Bridging the DMA and the GDPR - CIPL Comments on the Data Protection Implications of the Draft Digital Markets Act, December 6 2021; CIPL Paper – Limiting Legal Basis for Data Processing under the DMA, May 2023; CIPL Discussion Paper - Data Sharing Obligations Under the DMA: Challenges and Opportunities, May 13, 2024

innovation within the region. As Mario Draghi, Italian economist and ex-President of the European Central Bank, highlighted in his landmark report, excessive regulatory frameworks can stifle entrepreneurial activity and innovation and make it increasingly challenging for the EU to remain competitive. The EU now has approximately 100 tech-focused laws, including the new digital laws mentioned above. This encompasses various aspects of digital technology, data protection, and online platforms, and over 270 regulators are involved in some form of digital governance across EU Member States. This legislative forest discourages particularly small and medium-sized enterprises (SMEs) when faced with the high cost and complexity of navigating these rules. At present, the Draghi report sees the EU's innovation capacity and track record as lagging behind that of its global competitors, including the United States and China.[15]

15 Mario Draghi Report The Future of European Competitiveness.

III. Proliferation of consent requirements in the EU

The GDPR is clear that the free flow of data within the EU cannot be prohibited or restricted for data protection reasons[16] and that the protection of personal data cannot be placed above other fundamental rights protected in the Union.[17] The GDPR legislators recognised the transformative nature of technology for the economy and society[18] and enshrined in its recitals that "the processing of personal data should be designed to serve mankind".[19] As such, the GDPR, in addition to being a data protection law, can also be seen as an early piece of the Commission's digital strategy package towards "strengthen[ing] the data economy".[20]

Under the GDPR, to process personal data lawfully, organisations subject to it must be able to rely on one of six legal bases:

- individual consent (Art. 6 (1) (a)),
- contractual necessity (Art. 6 (1) (b)),
- legal obligation (Art. 6 (1) (c)),
- the protection of vital interest (Art. 6 (1) (d)),
- public interest (Art. 6 (1) (e)), and
- legitimate interest (Art. 6 (1) (f)).

These six legal bases allow organisations to choose the legal basis that is most appropriate to their particular processing activity. Importantly, there is no "preferred" legal basis under the GDPR;[21] they are all on equal footing with each other. However, the selection of a legal basis needs to be done with care as their suitability depends on the processing context and also may give rise to different individual rights.

Despite this parity between legal bases for processing and the dual objective of the GDPR to protect data and to enable digital transformation, there is an increasing trend by a number of data protection authorities (DPAs), including the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS),[22] to disregard the dual objective by elevating the protection of personal data above other fundamental rights, in the absence of efforts to strike a balance between competing interests or equities, and privileging consent as a basis for processing.

16 Article 1 GDPR.

17 Recital 4 GDPR.

18 Recital 6 GDPR.

19 Recital 4 GDPR.

20 Martin Nettesheim, *Data Protection in Contractual Relationships (Art. 6(1) (b) GDPR*, p. 15

21 See also Guidelines 1/2024 on processing of personal data based on Article 6(1) of GDPR, adopted 8 October 2024, which states that "*Art. 6 (1)(f) is one of six legal bases for the lawful processing of personal data envisaged by the GDPR. Article 6 (1)(f) GDPR should neither be treated as a last resort for rare or unexpected situations where other legal bases are deemed not to apply nor should it be automatically chosen ...*", p. 2

22 See recent decisions such as Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022. See also the letter from the EDPB to the European Commission concerning Guidelines on the Interplay between Digital markets act (DMA) and GDPR and EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive.

This trend is mirrored in some of the newly enacted digital legislation, and even the European Court of Justice (CJEU) seems to be leaning towards prioritising consent—presumably premised on the perception that consent is the most effective mechanism by which individuals can exercise control over their data in the digital economy.[23]

A. The decreasing acceptance of legal bases other than consent in judicial and regulatory decisions in the EU

In parallel to the proliferation of consent in existing or incoming digital legislation, we see a narrowing of other legal bases under the GDPR through interpretation by regulators and, to some extent, the CJEU, particularly with respect to legitimate interests and contractual necessity. This has resulted in diminishing options for lawful processing of data as well as legal uncertainty for organisations operating in the Union. Some recent examples include:

i. Bundeskartellamt Case

In the case of *Meta Platforms and Others v Bundeskartellamt*, the CJEU establishes the requirements for the lawful processing of third-party data by online social network operators by interpreting the legal bases of Article 6(1) of the GDPR in relation to personalised advertising. The Court in answering the questions referred by the German court, limited its analysis and judgement to the third-party data, without touching upon questions related to first-party data. The CJEU adopts a strict and literal approach to the contractual necessity legal basis, stating it must be "objectively indispensable" for a core contractual purpose and that there are no other workable or less intrusive alternatives.[24] This presents a departure from the GDPR, which merely requires that the processing is "necessary for the performance of the contract".[25] In order to demonstrate meeting the threshold imposed by the CJEU, organisations have to effectively show that the provision of their service cannot be achieved if the processing did not occur. The CJEU found that despite personalisation being useful to the user, they did not agree that personalised advertising was integral to providing a social media network. This interpretation effectively narrows the use of contractual necessity by disregarding the nature of the full business model, which is to provide the social media service without monetary fees in exchange for advertisement. This is concerning for modern data-driven organisations where personalisation and targeted advertising form a key part of their business, as it seems to require them to provide the service for free or charge a fee, where consent is not obtainable.

The Advocate General, in their Opinion, similarly encouraged a strict interpretation of the contractual necessity legal basis to ensure that organisations do not 'circumvent' the need for consent.[26] This interpretation overlooks the fundamental principle that the six legal bases under the GDPR are of equal status, without a hierarchy among them. In fact, the EDPB in their most recent draft guidance on the legal basis of legitimate interest under the GDPR specifically confirmed this and also clarified that there is no exhaustive or finite list of legitimate interests, and that therefore a broad range of interests are likely to qualify.

ii. EDPB Meta decisions

Prior to the Bundeskartellamt, in December 2022, the Irish Data Protection Commission handed down a decision to Meta Ireland based on a binding EDPB decision,[27] setting out that Meta cannot rely on contractual necessity Article 6(1)(b) as the legal basis for processing user data across its services for the purposes of personalised advertising.[28] The EDPB decision and

23 Martin Nettesheim, supra. 20, p. 26.

24 The CJEU recognises that *personalised content is beneficial for users, as it allows them to see content that largely matches their interests. However, the CJEU points out that "personalised content does not appear to be necessary in order to offer that user the services of the online social network". Rather, "those services may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services." Meta Platforms Inc and Others v Bundeskartellamt*, paragraph 102.

25 Article 6 (1) (b) GDPR.

26 AG Opinion, Meta Platforms Inc and Others v Bundeskartellamt, paragraph 51.

27 EDPB, "Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook Service (Art. 65 GDPR)," Adopted on December 5, 2022, available here.

28 Irish Data Protection Commission, "Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland," January 4th, 2023, available here.; EDPB, *"Facebook and Instagram Decisions: Important Impact on Use of Personal Data for Behavioral Advertising,"* January 12, 2023, available here.

the EDPB guidance[29] state that to rely upon the contractual necessity legal basis, organisations have to ensure the processing is "objectively necessary" to perform the contract. Objective necessity should include an assessment of the particular aim, purpose or objective of the whole service, including whether the reasonable data subject would expect the processing. The EDPB concluded in that case that personalised advertising was not objectively necessary to perform the contract and that the reasonable user would not expect their personal data to be used for personalised advertising.

The EDPB's decision did not look at the concrete case but EDPB argued in the abstract. It did not consider the concrete contract, which, based on the business model at that time was the provision of access to certain content without a monetary fee and supported by personalised advertisement.

It is interesting to note that the Irish DPA, in its initial draft decision, concluded that contractual necessity could, in principle, serve as an appropriate legal basis for Meta's services.[30] According to the Irish DPC interpretation, personalisation and personalised advertising can form a core part of the contract between Meta and Instagram users. The Commissioner noted that personalised advertising is one of the distinguishing factors of Instagram service and that an ordinary user would reasonably expect such functionality.[31] However, the position and analysis presented by the Irish DPC has been overruled by the European Data Protection Board. In October 2023, the EDPB further determined that Meta also could not rely on the legitimate interest legal basis under Article 6(1)(f) GDPR.[32] These decisions result in a more restrictive interpretation of legal bases listed in the GDPR, leaving consent as the sole valid legal basis for the processing of personal data for purposes of personalised advertising.[33]

iii. Consent in the context of data security and cybersecurity measures

This increased focus on consent also has an impact on the fundamental aspects of the functioning of the digital economy, such as strong cybersecurity measures or fraud prevention. All organisations must safeguard their operations, users, employees, customers, and partners from cybersecurity risks, unauthorised access, and other criminal activities. One of the most effective means of securing data is, for example, through the combination and cross-use of information across platform ecosystems, which significantly aids in identifying and preventing sophisticated cyber threats. However, the DMA specifically subjects such data processing practices to user consent, which introduces challenges for proactive security measures. Similarly, the *Bundeskartellamt* in Germany has held that: *"General and indiscriminate data retention and processing across services without a specific cause as a preventive measure, including for security purposes, is not permissible either without giving users any choice"*.[34] However, attempting to narrow the ability to scan for cybersecurity risks or fraudulent activity to instances where an initial concern (or "cause") is already present has the potential to significantly hamstring organisations' ability to act preventatively. Crucial security efforts could be undermined by effectively suggesting to ask bad actors for their consent for detection measures.[35]

29 European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, available here.

30 https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland

31 *Ibid* para 103.

32 EDPB, *EDPB Urgent Binding Decision on Processing of Personal Data for Behavioural Advertising by Meta*, November 1, 2023, available here.

33 Article 6(1)(a) GDPR and ePrivacy Directive (Directive 2002/58/EC).

34 Bundeskartellamt, Statement of objections issued against Google's data processing terms, available here.

35 CIPL White Paper - Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences, p.20.

IV. The limitations of consent

The inclusion of consent as one of the lawful bases under the GDPR reflects the fact that we live in a society which places value on individual choice. In wider society, consent forms part of the foundation of many crucial legal services such as in contracts, in marriage, or in real estate transactions. Consent under the GDPR is the method by which individuals can unilaterally grant or withdraw controllers' authority to use their personal data. The ability to consent or reject in appropriate situations gives individuals autonomy and control over their personal data. In order for individuals to truly gain autonomy over their personal data, their decisions to grant or withhold consent should be informed and voluntary and should be coupled with the ability to withdraw previously given consent at any time without detriment. Indeed, when individuals are asked to consent in a specific individual context, consent may be legitimate and useful.[36] However, the complexity of modern data processing operations calls the notion of reliable informed individual consent as the preferred legal basis into question for a number of reasons:

- **Consent is not scalable**: Individuals making a singular choice for each individual pre-defined purpose is outdated in the modern world
- **High burden on the individual**: The volume and complexity of information that individuals must read and digest to make an informed choice capable of protecting their rights and interests creates a disproportionate burden on them
- **Negative impact on third parties**: Certain processing activities that can have a significant impact beyond the individual should not be subject to one individual's decision

A. Consent is not scalable

Part of the motivation behind the European Commission's digital strategy acknowledges that data has not only commercial but also societal applications that may extend beyond its initial purpose for collection or generation[37]. In other words, there may be new uses for previously collected data that may be beneficial for society. These new uses may not always be evident at the time of initial collection or creation, when consent would have to be obtained, i.e., prior to processing. Recital 33 GDPR recognises this issue to some extent for scientific research and suggests allowing individuals to provide consent on a less granular level where sufficient safeguards (ethical standards and technical and organisational measures in accordance with Article 89 (1) GDPR) are present. Allowing for a broader opt-in to wider use cases framed by accountability measures, such as an ethical standard and security measures to safeguard the individual's rights, should provide an appropriate approach to enabling the benefits of the digital revolution while protecting stakeholder rights.

Nonetheless, the EDPB and the EDPS assert that obtaining consent for "general interests" beyond scientific research (as exemplified in the context of data altruism in the context of the DGA) would not align with the GDPR unless an exhaustive list for such additional purposes is provided.[38] However, technology is dynamic and constantly evolving. Similarly, data possesses

36 Neil Richards and Woodrow Hartzog, "The Pathologies of Consent", 96 Washington University Law Review 1461, 2019.

37 Recital 6 Data Governance Act.

38 EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act).

multiple dimensions, influenced by factors such as its context, the intended recipient, timing, and whether it will be enriched with additional data. All these elements contribute to its utility, which may only gradually unfold as technology advances and matures.[39] Requiring a finite enumeration of possibilities inevitably limits future applications and risks becoming quickly outdated. The idea of a singular use of data for a specific pre-defined purpose, where the individual is duly informed and then makes a single choice, is no longer reflective of the complexity of the modern digital environment. The concept of single consent is non-scalable.

In addition, the fact that consent can be withdrawn at any time adds to the overall complexity. For example, the right to withdraw consent may place an individual with a private health insurance contract in a position to withdraw his or her consent to data processing. The insurer is then, effectively, no longer able to fulfil the contract, as it necessitates processing health data (which is subject to consent under Article 9 GDPR).[40]

B. Disproportionate burden on the individual

To be sufficiently "informed" to provide valid consent under GDPR, individuals must be given essential information on all processing operations and their purposes.[41] As a result, consent forms have become extremely challenging[42] due to the complexities of modern processing realities. Even the best-designed consent forms, presented in "intelligible and easily accessible form, using clear and plain language" as required by Recital 42 GDPR, must reflect all processing operations and types of personal data processed, making them unnecessarily long.

Additionally, the sheer number of consent forms presented to individuals throughout the day makes it impossible to satisfy them all without reducing them to mere box-ticking exercises.

Researchers have found that it would take 76 work days per year for a person to read all of the privacy policies they are confronted with[43]. As Richards and Hartzog put it, "we have over-used the tool of consent to the point that it has become badly damaged".[44]

The European Commission acknowledged this challenge of consent fatigue in the context of its Cookie Pledge Initiative.[45] The Commission proposed several pledging principles in an effort to limit some of the consent requests while still empowering consumers to make informed choices. The initiative ultimately did not succeed to reconcile the goal of simplification with the stringent existing legal framework of the ePrivacy Directive and GDPR.[46]

C. Negative impact of individual consent decisions on third parties: data security and fraud prevention

Digital products and services often interact, involving exchanges of user data with an impact on more than one person. Similarly, the actions of one individual on a platform may affect a number of other individuals. The concept of consent is based on the idea of the individual exercise of choice, but in the digital context, it invariably touches on the rights of third parties, be it the platforms or other users.[47]

This becomes very clear in the context of fraud prevention and cybersecurity measures. As mentioned earlier, Art. 5(2)

39 See also Data Policy: A Conceptual Framework, p. 3.

40 CIPL Paper "The First Six Years", p. 18.

41 Guidelines 05/2020 on consent under Regulation 2016/679, para 64.

42 Daniel J. Solove, in *"Murky Consent: An Approach to the Fictions of Consent in Privacy Law,"* 104 Boston University Law Review 593 (2024), calls it "an exercise in torturous tedium", page 24.

43 Privacy Policies Are Difficult to Read.

44 Neil Richards, Woodrow Hartzog, supra n.40.

45 https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en; https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-reply-commissions-initiative-voluntary-business-pledge_en.

46 Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities available here.

47 Nettesheim, supra n.20 p. 31.

DMA has the potential to make cybersecurity and fraud prevention measures subject to consent.[48] Similarly, as indicated above, the German *Bundeskartellamt* has suggested that general prevention measures should also be subject to consent.[49] In both instances, this would ultimately mean requiring malicious actors' consent for data processing designed to detect their malicious activities. It is obvious, though, and even legally required, that organisations must protect themselves and their business partners or end users from security intrusions, unauthorised access, fraud, and cyberattacks. Requiring prior consent could disrupt the proper functioning of digital services and negatively impact third parties.[50] Recital 49 GDPR makes it clear that processing for network and information security is a legitimate interest of a data controller. Some processing decisions should not be "solely the subject of one party's mercurial free will".[51]

48 See our analysis above on p. 11.

49 *Ibid*.

50 CIPL White Paper - Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences

51 Nettesheim, supra n.20, p. 31

V. The role of legitimate interest and contractual necessity under the GDPR

The apparent privilege of consent goes hand in hand with a more conservative interpretation of the GDPR's other legal bases, which has led to reticence in the marketplace to make use of them.[52] This stands in direct conflict with the fact that the GDPR provides numerous legal bases without preference for one over the other.[53]

An overly restrictive interpretation of the other bases may result in organisations trying to rely on consent, even where it would be more appropriate to rely on legitimate interests or contractual

necessity. This can result in organisations considering not proceeding at all, including in cases that involve innovative data uses with little or no risks to individuals. For instance, during the COVID-19 pandemic, private organisations were unclear on whether they could rely on public or legitimate interests to conduct related data analytics and research for their processing in response to the pandemic.[54]

While the recent decision by the European Court of Justice confirming that commercial interests can indeed be considered "legitimate" in the sense of Article 6 (1)(f) GDPR was an important milestone,[55] there continues to be uncertainty around the applicability of the legitimate interest legal basis for the purpose of training AI in Europe. This has been subject to a number of consultations by data protection authorities in Europe.[56]

A. Contractual Necessity

The contractual necessity legal basis provided by the GDPR allows organisations to process personal data for the performance of a contract or in order to take steps at the request of the individual prior to entering into a contract. However, the EDPB and the CJEU have interpreted the contractual necessity legal basis restrictively by setting a high bar for its use. However, the contractual necessity legal basis could benefit both organisations and individuals.

Key features and benefits of the contractual necessity legal basis

The contractual necessity legal basis enhances digital autonomy

- One of the main arguments in favour of using contractual necessity is that it enhances digital autonomy. Contracts have the ability to empower individuals to choose what data they want to share in exchange for a service. For example, individuals may enter into a contract with an organisation in order to get free access to their online services, which otherwise would have come at a cost to the user. Giving users the ability to enter into genuine contracts allows individuals to conclude mutually beneficial contractual agreements regarding the use of their data, enhancing digital autonomy.[57]

52 CIPL Report "The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement", available here.

53 EDPB Guidelines 1/2024, p. 4

54 CIPL Paper How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, p. 5

55 In Case C-621/22, Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens, para 38-40, the Court confirmed that a wide range of interests could be regarded as legitimate. The interests do not have to be enshrined in and determined by law; however, they must be lawful.

56 CIPL responded to the ICO and the CNIL, respectively.

57 Martin Nettesheim, *Data Protection in Contractual Relationships (Art. 6(1) (b) GDPR*, p. 50.

The contractual necessity legal basis ensures clarity for the individual

- The contractual necessity legal basis by its very nature requires the existence of a contract which is clear in substances and contains a fundamental objective. Where an organisation relies on this legal basis, it is required to define the scope of its processing in the contract which in turn is governed by robust domestic contract law. This provides the individual with clarity as to the activities of the organisation and legal certainty regarding their rights.

The contractual necessity legal basis is set within wider contractual law which offers protections

- In addition, existing domestic laws already offer protections that promote material contractual autonomy. Contract law addresses issues such as transparency, information asymmetry, power imbalances, and the use of unfair clauses. These protections help ensure that contracts represent a genuine and balanced agreement between the parties involved.[58] The high bar set by the EDPB, in particular, limits the utility of this legal basis in the context of the digital economy.

B. Legitimate Interest

Some of the reservations that have been expressed regarding the legitimate interest legal ground often fail to recognise that this legal ground is actually accompanied by robust accountability and risk assessment obligations, delivering real protection for individuals.[59]

Key features and benefits of the legitimate interest legal basis

The legitimate interest legal basis relies on strong organisational accountability

- The GDPR is an accountability-based law which requires organisations to take steps to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls. This is coupled with the organisation's ability to demonstrate the existence and effectiveness of such actions and controls internally and externally. The legitimate interest legal basis under the GDPR relies on the accountability principle. In order to rely on it, organisations have to conduct a balancing test assessing the potential risks and competing individual interests, rights and freedoms related to a processing operation and define measures to mitigate the risks. Moreover, organisations have to document such assessments and be able to demonstrate the outcomes.

The legitimate interest legal basis is a reflection of a risk-based approach, which benefits both organisations and individuals

- The GDPR's risk-based approach is inherent to the legitimate interest legal basis. Organisations can only rely on this legal basis when the processing is necessary for the stated legitimate interest and does not result in a risk of harm to individuals. It requires organisations to undertake the necessary risk assessments, define the mitigation measures, train employees on risks and mitigation measures, monitor the continued effectiveness of the mitigations, identify potential compliance gaps, fix them and continuously improve the level of protection. The legitimate interests assessment can form part of the overall risk assessment practices.

The legitimate interest legal basis is contextual and relies on a case-by-case assessment

- The legitimate interests assessment is linked to a processing activity in a specific context. Thus, its results are not set in stone and may vary according to the nature of the processing activities, the likelihood and severity of harm to individuals, the mitigation measures implemented by organisations, and individuals' reasonable expectations. Therefore, it is important to not pre-suppose that certain types of personal data and data processing activities would be inherently unfit for the legitimate interest legal basis without undertaking a case-specific risk analysis.

58 Ibid, 58.

59 See CIPL White Paper "How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation" and CIPL Legitimate Interest Paper - CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data.

The legitimate interest legal basis covers a non-exhaustive list of processing activities and offers flexibility, which is necessary for complex uses of data

- The legitimate interest legal basis is not limited to specific processing operations. It may cover everyday, routine, and established business purposes like fraud prevention and cybersecurity, as foreseen in recitals 47 and 49 GDPR, provided that the specific processing can pass the requisite balancing test. At the same time, it may also cover more complex, unique, innovative, original or new data processing activities that are key for innovation and for the development of the digital economy, if they pass the requisite balancing test. For example, the legitimate interest legal basis can be instrumental for AI training in the context of developing new large language models, and in many cases, may be the only available legal basis for algorithmic training.[60]

The legitimate interest legal basis provides strong protections to individuals

- The legitimate interest legal basis provides an opportunity for individuals to object at any time to the processing of their personal data. Relying on this legal basis also requires organisations to enhance transparency about the data processing and, as mentioned above, to document and demonstrate the outcome of the legitimate interest assessment.[61]

The flexibility provided by the legitimate interest basis, coupled with organisational accountability and a risk-based approach, therefore, makes it a crucial enabler of responsible innovation and an accountable digital economy.[62] It is, therefore, a positive development that EDPB, in a recent guideline, expressly acknowledges that "legitimate interest" under the GDPR should not be seen as *a "last resort"* for rare or unexpected situations where other legal bases are deemed not to apply.[63] This will be particularly important in the context of the continued development of AI technology.[64]

60 See CIPL response to the CNIL How-To Sheets on the Development of Artificial Intelligence Systems, available here. In the submission CIPL agrees with the CNIL's assertion that legitimate interests should be understood broadly. In addition, CIPL highlights that the Recital 47 GDPR non-exhaustive list should include the development of AI systems as an example of a legitimate interest, p. 3.

61 Ibid, para 44. The legitimate interest legal basis requires controllers to balance the opposing rights and interests based on a case-by-case assessment. Under Article 21 GDPR, the controller has the ability to demonstrate compelling legitimate grounds that may override the individual's objections or where the continued processing is for the defense of a legal claim.

62 CIPL White Paper - How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, available here.

63 EBPB Draft Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 2, available here.

64 See CIPL Response to the ICO's Fifth Consultation on Allocating Controllership Across the Generative AI Supply Chain, October 2. 2024; and CIPL Response to CNIL How-To Sheets on the Development of Artificial Intelligence Systems, October 1, 2024.

VI. Beyond consent: Moving away from consent and empowering the use of other legal bases

Globally, there is also a recognition of the limitations of consent and the necessity to adapt to the reality of the digital environment.

a. Since leaving the EU, the UK government, for instance, has proposed changes to the existing UK data protection framework in order to promote innovation and responsibly ease the burden of compliance for organisations. The proposed amendments considered creating a list of acceptable use cases where organisations could rely on the legitimate interest legal basis such as the purposes of crime and fraud prevention, the safeguarding of children and in a public emergency. While the reform did not pass due to changes in Government, there still remains a strong commitment to reforming the UK GDPR to support innovation.

b. In the US, representatives of the Federal Trade Commission have expressed some doubts on the continued effectiveness of the notice and choice model of consent.[65]

c. Singapore amended its data protection framework,[66] introducing broader exemptions to the general requirement to obtain consent, including where processing was in the organisation's legitimate interests.

   Under the legitimate interests exception in Singapore, organisations are now able to process personal data without obtaining consent, as long as it is within their legitimate interests and they conduct a balancing exercise on adverse effects to the individual. The amended data protection law also introduced a business improvement exception, whereby organisations do not need to obtain consent when they are improving their services, developing new goods, for analytics or for personalisation. The amendments also introduced the concept of "deemed consent", where individuals can be 'deemed' to have given consent in certain situations. Individuals may be deemed to have consented to further processing if they have been notified in advance of the processing, in which case organisations will have to conduct a balancing test to ensure there is no adverse effect on the individual and ensure that their notification and opt-out period is adequate. Furthermore, where organisations share personal data where it is reasonably necessary to conclude or perform the contract between organisations, the individual may be deemed to have given consent for the processing of personal data.

65 MLEX interview with Samuel Levine, *"Comment: FTC consumer protection chief Levine sees 'paradigm shift' in US privacy enforcement,"* August 2, 2023, available here [behind a paywall]. The article notes that: "The regulator is moving away from a strict reliance on the "notice and choice" regime in which US companies typically could use personal data freely for advertising or other purposes, so long as they disclosed those practices and gave consumers the choice to opt out".

66 Personal Data Protection (Amendment) Act 2020.

d. Canada has also proposed amendments to its data protection framework[67] introducing a number of different exemptions for consent when collecting, using or disclosing personal information in the draft Consumer Privacy Protection Act. One of these exceptions is framed similarly to the legitimate interest ground for processing under the GDPR: Section 18 of the draft law provides that an organisation may collect or use an individual's personal information without consent.[68] This is possible in cases where the collection or use is made for a business activity, and a reasonable person would expect such a collection or use for that activity, and the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

67 Bill C-27, presented 2022.

68 https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E

VII. Rethinking EU's Digital Strategy: Towards a more balanced approach

The EU's recent digital strategy, while intended to boost the data economy, presents challenges due to its over-reliance on consent as a legal basis for data processing. Although consent is one of the cornerstones of expressing individual autonomy, its broad application often leads to *"consent fatigue"*, as individuals face excessive and complex requests that undermine their ability to make informed decisions. These limitations not only strain user autonomy but also diminish the efficiency of digital ecosystems.

- The proliferation of consent requirements in digital laws like the DMA, DSA, and DGA, combined with a restrictive interpretation of alternative legal bases, such as legitimate interests and contractual necessity by regulators and the Court of Justice, are creating an unbalanced regulatory landscape. This trend is leading to consent becoming the default, even in situations where it might not be the most appropriate or effective solution.
- Consent in the digital world has three key limitations:
  - Scalability: Consent, based on individual choice for specific, pre-defined purposes, struggles to keep pace with the evolving nature of data and its uses in the digital economy.
  - Burden on Individuals: The complexity and volume of information required for informed consent creates a disproportionate burden on individuals, leading to consent fatigue and potentially uninformed decisions.
  - Impact on Third Parties: Individual consent decisions can negatively impact essential functionalities like cybersecurity, fraud prevention, and data-driven innovation, which often involve processing data with implications beyond the individual.

In contrast, legitimate interest (LI), when combined with robust accountability and risk assessment, offers a more flexible and balanced approach. It empowers organisations to process data for purposes beyond the initial point of collection while ensuring individual protection through transparency, the right to object, and a contextual risk-based approach. Similarly, contractual necessity, rooted in clearly defined agreements between parties, can foster digital autonomy by allowing individuals to choose how their data is used in exchange for services.

The experiences of jurisdictions like the UK, the US, Singapore, and Canada highlight a global shift away from strict reliance on consent towards a more balanced approach recognising the value of LI and contractual necessity in enabling responsible data processing.

This evolving landscape holds valuable lessons for South Korea as it implements amendments to its Personal Information Protection Act (PIPA). While the move towards greater reliance on contractual necessity is positive, it is crucial for the PIPC to provide clear guidelines on its application, particularly in areas like targeted advertising and biometric data collection. Furthermore, embracing legitimate interest as a valid legal basis, in line with global trends, can further empower responsible innovation and ensure the sustainable growth of South Korea's digital economy.

VIII. Developments in South Korea: what could be the lessons learned from the developments in Europe?

In South Korea, the processing of personal information is primarily governed by the PIPA and its implementing regulation, the Enforcement Decree of the PIPA.

Previously, businesses heavily relied on obtaining consent as the legal basis for processing personal data rather than other grounds such as contractual necessity or the legitimate interest of the data controller. This reliance was largely due to the burden of demonstrating the necessity required by these alternative legal bases.

However, with the recent amendment to the PIPA, which took effect on March 15, 2024, consent may no longer serve as the primary legal basis for data processing because businesses are no longer required to prove "inevitable necessity" for processing personal data in contractual contexts. The amended Article 15(1)(4) now allows processing where it is simply "necessary" to (i) perform a contract between the data subject and data controller or (ii) take measures requested by the data subject during the course of entering into such a contract. An example of (i) is when an online shopping platform receives a product order from a customer and processes personal data, such as the customer's address, contact details, and payment information, to fulfil the contract—this includes handling payment processing, delivery, and after-sales service. An example of (ii) is when a company collects and processes personal information, such as resumes, graduation certificates, and academic transcripts from job applicants, as part of the process before establishing an employment contract.

Along with it, amendments to the PIPA Enforcement Decree were passed last year, which came into effect on September 15, 2024. The most notable part of these amendments is bringing the requirements for valid consent under the PIPA closer to the consent scheme of the GDPR by removing the previous distinction between mandatory and optional consent, which in turn favours a "free-will consent" approach.

Prior to the amendment of PIPA Enforcement Decree, businesses were required to obtain "optional" consent separately from "mandatory" consent. However, "mandatory consent" implied that the data subject must provide consent, inherently conflicting with the notion of "consent given under free will." Recognising this conceptual conflict, the PIPC is shifting away from the 'mandatory vs. optional' consent regime for processing personal data and attempting to render the other legal bases more widely usable. Under the GDPR, legal grounds for processing personal data – such as consent, contractual necessity, and legitimate interest – are all regarded as holding equal status. While South Korea's previous regime emphasised consent, these changes open new avenues for processing data under other legal grounds, potentially reducing the reliance on consent.

In certain respects, mandatory consent—which previously allowed service providers to require consent on the grounds that it was necessary for the provision of a service—must now be justified under either contractual necessity or legitimate interest. When applied to targeted advertising, the PIPC has traditionally held that this type of advertising should not be subject to mandatory consent (i.e., service providers cannot compel users to agree to receive targeted ads). With the removal of the mandatory consent mechanism, questions may arise on whether targeted advertising can now rely on contractual necessity or legitimate interest.

Digital services are evolving at an unprecedented pace, with many providers now analysing user activity to refine their offerings and introduce new features. In particular, a growing number of digital services rely on analysing personalised advertising to deliver content aligned with individual preferences, making this a core aspect of the service itself. Without such personalisation (i.e., personalised advertising), users are more likely to encounter only the most popular content, potentially missing out on material more closely aligned with their interests that might otherwise go undiscovered. Essentially, free services enjoyed by users are funded by advertisers. Providing free services is possible when businesses are able to use the personal data collected from users to provide personalised ads that are relevant and of interest to their user. As does any other bilateral contract, a fair value trade-off has been established between the users and service providers in the status quo.

Beyond personalised advertising, there are cases where optional consent alone may not be practical. In large apartment complexes across South Korea, registering residents for access to community facilities often requires the collection of personal information. Using access keys alone poses security risks, as they can be borrowed, potentially allowing unauthorised individuals into restricted areas. To address this issue, collecting biometric data for secure access may become essential. These situations, once managed through mandatory consent, now could fall under contractual necessity or legitimate interest.

However, clear guidelines on this shift are still limited, creating some uncertainty for businesses. As in the *Bundeskartellamt* case, where the CJEU strictly interpreted contractual necessity and Facebook's legitimate interest, South Korea's PIPC could similarly take a restrictive approach and reject the applicability of contractual necessity for using third party data for personalised advertising. The future of many businesses, whose core business models rely on personalisation and personalised advertising, depends on how the PIPC interprets this issue.

Moreover, the shift from the "mandatory vs. optional" consent regime may introduce interpretative challenges for businesses, especially in specific scenarios. For instance, prior to the amendment, the overseas transfer of data for purposes of entrustment did not require consent, regardless of whether the entrustment was for marketing purposes. Under the amended framework, however, does this exemption still apply when the transfer is intended for marketing-related entrustment? Following the amendment, it appears that only overseas entrustments deemed essential for contractual obligations are exempt from consent requirements. This, however, is contingent on how the term "contractual necessity" is interpreted in the context of overseas data transfers. Given the historical backdrop of the PIPA amendments and established industry practices, relying on optional consent when entrusting personal data to overseas entities for transmitting marketing messages seems impractical. As such, the recent amendments to the PIPA Enforcement Decree are likely to raise concerns in unforeseen areas of business operations.

In light of these shifts, the amended PIPA framework reflects a significant move towards a more flexible landscape. By expanding the applicability of contractual necessity and legitimate interest, South Korea's data protection regime allows for a nuanced approach that supports innovation while safeguarding user rights. As the world's digital economy is heavily reliant on personal data to deliver personalised experiences, the ability to process data under these legal grounds will be crucial for sustaining service relevance and competitiveness in a rapidly evolving digital economy. Moving forward, a balanced application of these new standards—paired with ongoing regulatory guidance—will be essential to ensuring that data-driven services can continue to flourish without compromising the foundational principles of privacy and user autonomy.

Recommendations

In the context of the amendments to PIPA in South Korea, we draw attention to:

- Jurisdictions worldwide should be cautious about replicating data protection concepts and policies established under the EU framework. Although the EU is recognised for having one of the most comprehensive data protection frameworks, there are notable limitations and negative impacts on the digital economy that should be examined with caveats and thorough considerations.

- PIPC should clarify that they will maintain their current consent practices concerning mandatory versus optional consent. This approach has proven workable for businesses thus far.
- Furthermore, it is encouraged that the PIPC continue to explore the possibility of relaxing alternative legal bases to facilitate reasonable data processing activities, such as legitimate interests or contractual necessity. When assessing the alternative legal bases, it is imperative that the regulator takes a holistic approach, taking into account (i) the wider context a certain processing activity is taking place, including the economic reality of a contractual relationship between service providers and their users; and (ii) a consideration the essential nature of certain data for a service to be provided, instead of trying to carve out a formalistic approach.

Annex - Proliferation of legislative consent requirements in the EU

The list below provides an overview over some of these recent legislative developments[69]:

Digital Markets Act (DMA)

- **Article 5(2) Data combination and cross-use of data** – prohibits data combination and the cross-use of personal data among gatekeeper services, unless the end user has given GDPR consent. The DMA has three other legal bases under Article 6 GDPR, namely (i) compliance with a legal obligation, (ii) protection of the vital interest of the data subject or another natural person, or (iii) necessary for the performance of a task in the public interest, but explicitly denies legitimate interest or contractual necessity.[70]

Digital Services Act (DSA)

- **Article 26 (3) Advertising on online platforms** – Providers of online platforms shall not present advertisements to recipients of the services based on profiling using special categories of personal data under the GDPR.
- **Recital 68** – The requirements relating to advertising are without prejudice to the application of the relevant provisions of GDPR, in particular, the need to obtain **consent** of the data subject prior to the processing of personal data for targeted advertising.

Digital Governance Act (DGA)

- **Article 5(6) Conditions for Re-use** – Where the re-use of data cannot be allowed due to the absence of a secure processing environment and if there is no legal basis for transmitting the data under the GDPR, the public sector body shall make best efforts to provide assistance to potential re-users in seeking the **consent** of the data subject whose rights and interests may be affected by such re-use.
- **Article 25 European data altruism consent form** – The Commission may develop a European data altruism consent form to facilitate the collection of data based on data altruism which shall allow the collection of consent across Member States. Where personal data is provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a specific data processing in compliance with the GDPR.
- **Recital 54** – Typically, data altruism would rely on the **consent** of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of the GDPR.

69 See also CIPL Infographic 'A Day in the Life: Data Consent' which effectively articulates an example of a daily user journey and how this interacts with multiple legislative acts which prompt user consent.

70 CIPL White Paper - Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences, available here.

ePrivacy Directive and proposed ePrivacy Regulation (EPR) To replace the ePrivacy Directive

ePrivacy Directive and the EDPB Guidelines on the technical scope of Art. 5(3) ePrivacy Directive

- The ePrivacy Directive requires individual **consent** primarily in situations involving the storage of or access to information on a user's device. For example, consent is required in the following circumstances: cookies and similar technologies, direct marketing communications, location data, etc. However, the recently adopted EDPB Guidelines on the interpretation of Art 5(3) ePrivacy Directive significantly expand the scope of notions of 'gaining access', 'stored information' and 'terminal equipment', which, as a result, would leave little if any communication over the internet outside the scope requiring individual **consent**.[71]

Proposed ePrivacy Regulation – to replace the ePrivacy Directive

- **Article 6 Permitted processing of electronic communications data** – providers of electronic communication services may process electronic communications:
- **Art 6(2)(c) Metadata** – If the end-user gives consent for one or more specified purposes provided that the purposes concerned could not be fulfilled by processing information anonymously.
- **Art 6(3)(a) and (b) Content** – if all end-users give **consent** for one or more specified purposes that (a) relevant service cannot be fulfilled without the processing of such content, or (b) cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority.
- **Article 8(1) (b) Protection of information stored in and related to end-users' terminal equipment** – the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is prohibited except (b) the end-user has given his or her **consent**.
- **Article 10 Information and options for privacy settings to be provided** – (1) Software placed on the market permitting electronic communication shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. (2) Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.
- **Article 15 Publicly available directories** – the providers of publicly available directories shall obtain the consent of end-users to include their personal data in the directory (...).
- **Article 16 Unsolicited communications** – natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons who have given their **consent**.

Revised Payments Services Directive (PSD2)

- **Article 64 Consent and withdrawal of consent** – Requires explicit **consent** from the payer for a transaction to be executed, which can be withdrawn at any time until the moment it has been received by the payment service provider.

71 See CIPL Response to the EDPB Public Consultation on Draft Guidelines 02/2023 on the Technical Scope of Art. 5(3) of the ePrivacy Directive, which examines in detail the impact of proposed changes to the interpretation of Art. 5(3), available here.

About

Centre for Information Policy Leadership (CIPL)

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world.

For more information, please see CIPL's website at **www.informationpolicycentre.com**

Bae Kim & Lee (BKL)

Established in 1980, BKL is a leading full-service law firm in Korea. As one of the largest law firms in the country, BKL is composed of approximately 800 professionals, including lawyers qualified in Korea and foreign jurisdictions, accountants, patent attorneys, and other qualified specialists and advisors. BKL offers expertise across a full range of practice areas, including corporate/M&A, foreign investment, finance, fair trade and competition, regulatory matters, labor and employment, tax, intellectual property, real estate and construction, criminal matters, litigation, dispute resolution, and arbitration. BKL's experts work collaboratively to anticipate client needs and deliver practical solutions, enabling clients to focus on managing their businesses.

For more information, please visit BKL's website at **www.bkl.co.kr**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

24558.1224